Infrastructure Sécurisée Linux

Said HASHEMI

Objectif du projet

L'objectif de ce projet est de mettre en place une infrastructure réseau sécurisée sous Linux Debian 12 en environnement virtualisé (VMWare Workstation ou VirtualBox).

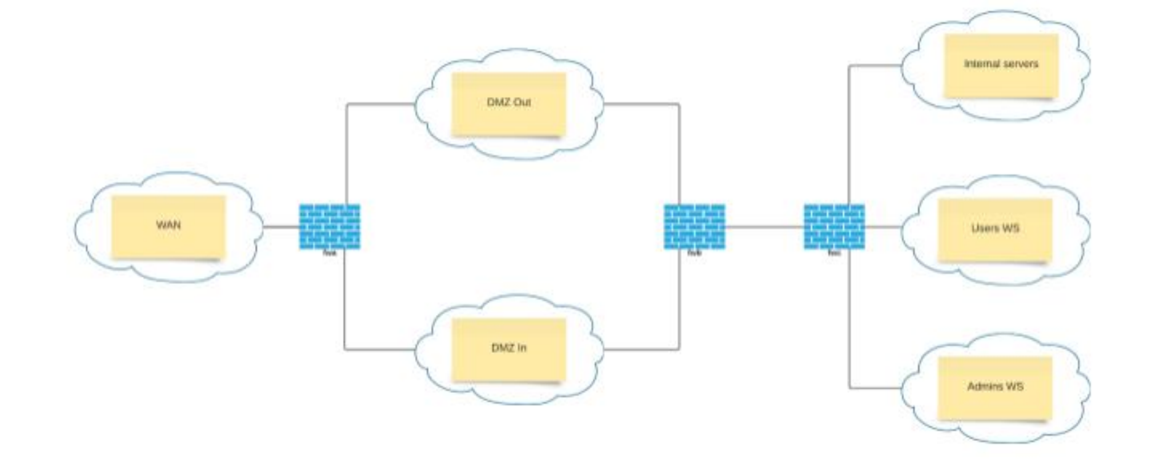
Les technologies clés déployées incluent :

- ❑Filtrage avec IPTables
- ❑Gestion DNS avec Bind9
- ❑DHCP via Kea DHCP
- ❑Routage avec FRR Routing
- ❑Serveur web Apache2 ou NGINX
- ❑Serveur de logs centralisé (Syslog-NG ou RSyslog)
- ❑Proxy Squid et Reverse Proxy

Schéma logique du réseau

Le schéma réseau inclut plusieurs segments :

- ❑WAN
- ❑DMZ In
- ❑DMZ Out
- ❑Internal Servers
- ❑Users WS
- ❑Admins WS



Des pare-feux (FWA, FWB, FWC) assurent la sécurité et l'isolation entre ces différentes zones.

Choix du virtualiseur

Virtualiseur choisi : VMware Workstation

- ❑Stabilisé et adapté aux infrastructures complexes
- ❑Installation de Debian 12 sans environnement graphique pour optimiser les ressources

Adressage des équipements intermédiaires

Chaque pare-feu dispose de plusieurs interfaces réseau configurées de manière sécurisée :

- **FWA** : WAN (DHCP), DMZ In (10.0.0.1/11), DMZ Out (10.32.0.1/11)
- **FWB** : Vers FWC (10.128.0.1/30), DMZ In (10.0.0.2/11), DMZ Out (10.32.0.2/11)
- **FWC** : Vers FWB (10.128.0.2/30), Internal Servers (10.64.0.1/12), Users WS (10.80.0.1/12), Admins WS (10.96.0.1/12)

Routage avec FRRouting

FRRouting a été installé et OSPF activé pour assurer la connectivité entre les différentes zones.

Exemple sur FWC:

```
fwc# show ip ospf route
============ OSPF network routing table ============
N    10.64.0.0/12          [100] area: 0.0.0.0
                           directly attached to ens34
N    10.80.0.0/12          [100] area: 0.0.0.0
                           directly attached to ens35
N    10.96.0.0/12          [100] area: 0.0.0.0
                           directly attached to ens36
N    10.128.0.0/30         [100] area: 0.0.0.0
                           directly attached to ens37

============ OSPF router routing table =============

============ OSPF external routing table ===========
```

Filtrage IP Tables

Objectif : Protéger l'infrastructure contre les accès non autorisés.

- ❑**FWC :** Autorisation du trafic interne et filtrage stricte entre DMZ et réseaux internes
- ❑**FWB :** Communication contrôlée entre DMZ-In et DMZ-Out
- ❑**FWA :** Filtrage du trafic entrant depuis le WAN

Les règles sont sauvegardées via **iptables-save** et **iptables-persistent**.

DNS et DHCP

❑**Bind9 :** Serveur DNS interne

❑**DHCP (Kea DHCP) :** Attribution automatique des adresses IP

❑**Tests :** Nslookup et validation DHCP

```
root@fwc:~# systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-10 10:28:55 CET; 3h 19min ago
       Docs: man:named(8)
   Main PID: 2227 (named)
     Status: "running"
      Tasks: 8 (limit: 1035)
     Memory: 11.5M
        CPU: 978ms
     CGroup: /system.slice/named.service
             └─2227 /usr/sbin/named -f -u bind
```

```
root@fwc:~# systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
     Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
     Active: active (running) since Mon 2025-02-10 10:33:46 CET; 3h 16min ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 1 (limit: 1035)
     Memory: 3.2M
        CPU: 89ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─2832 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens34
```

Proxy Squid

- Installé sur **FWC** pour filtrer et contrôler le trafic web.
- Tests effectués pour garantir son bon fonctionnement.

```
root@fwc:~# dpkg -l | grep squid
ii  squid                     5.7-2+deb12u2
ii  squid-common              5.7-2+deb12u2
ii  squid-langpack            20220130-1
```

Test :

```
root@interne:~# curl -x http://10.128.0.2:3128 -L https://www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="fr">
images/branding/googleg/1x/googleg_standard_color_128dp.png" itemprop="image"><ti
5BdGC7M8P1P776AU',kEXPI:'0,3700260,689,435,538661,2872,2891,43028,30022,16105,344
4189,10898,15164,8181,5937,4556,3894,56130,585,6751,23879,9140,4598,328,6226,7974
,6764,3,2,5823,1498,3854,41,13639,1,1443,4095,1203,2895,1210,302,4156,3887,15837,
41,2,415,4024,637,172,6,359,789,714,639,2,209,918,1275,55,525,281,218,1,319,328,1
,35,1273,217,1223,955,354,1029,15,139,3,2810,4,5,404,810,541,14,8,826,6,1553,900,
58,3,818,394,497,11,1,346,21,169,361,1112,273,2,735,581,1046,124,973,476,123,154,
9,307,22,6,60,440,164,293,8,1,1,3,569,44,1003,39,1011,151,153,92,141,388,173,42,4
,8018905',kBL:'9Rrr',kOPI:89978449};(function(){var a;((a=window.google)==null?0:
hp';google.kHL='fr';})();(function(){
```

Reverse Proxy (Nginx)

- Mise en place d'un reverse proxy pour sécuriser l'accès aux services web internes.
- Tests effectués avec accès aux applications internes.

```
root@fwc:~# dpkg -l | grep nginx
ii  nginx                                   1.22.1-9
ii  nginx-common                            1.22.1-9
```

Le retour de la commande curl « 200 OK » signifie que reverse proxy fonctionne correctement

```
root@fwc:~# curl -I http://localhost
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Mon, 10 Feb 2025 15:19:34 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Mon, 10 Feb 2025 10:21:37 GMT
Connection: keep-alive
ETag: "67a9d331-267"
Accept-Ranges: bytes
```

Syslog (Centralisation des logs)

- Serveur de logs configuré avec **Syslog-NG** pour récupérer et analyser les logs.
- Tests effectués pour valider la collecte centralisée des journaux.

Au titre d'un exemple, logs des services de système :

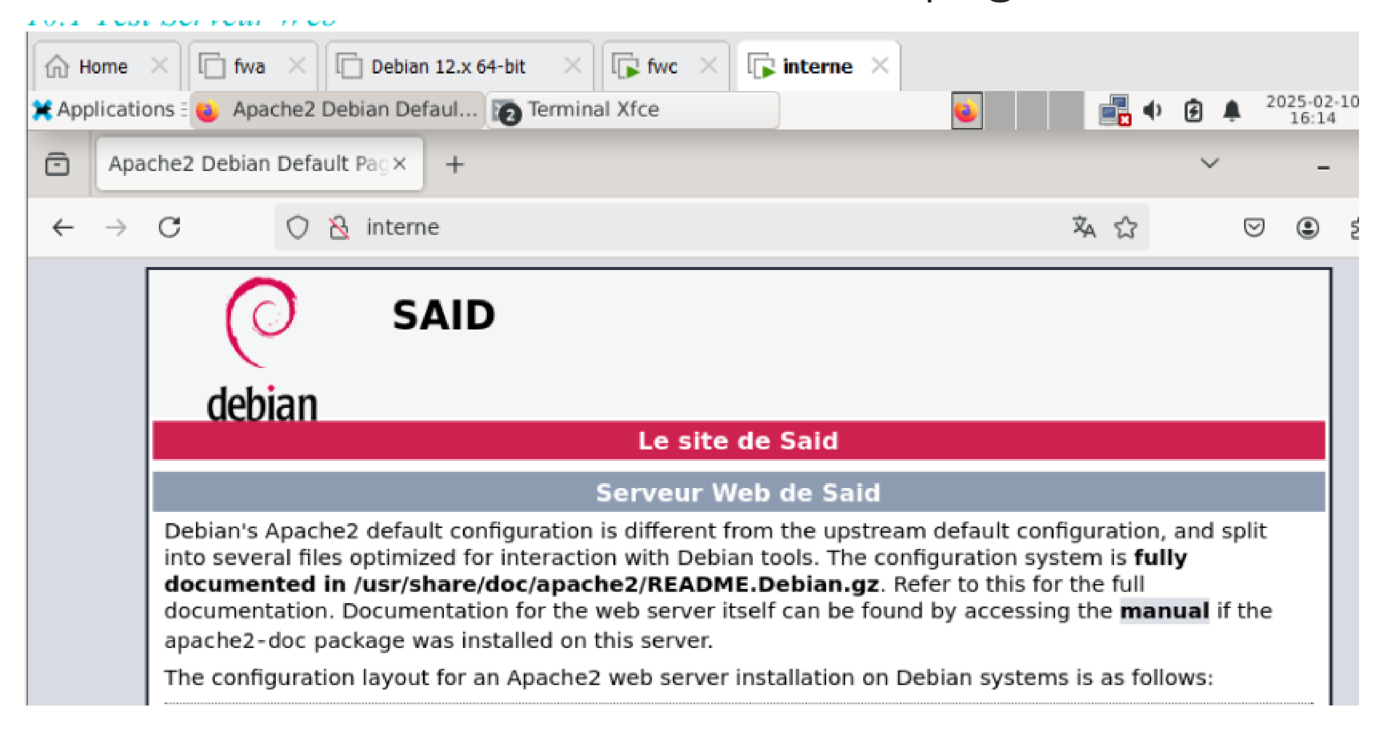
```
Oct  5 10:55:01 debian dbus-daemon[1234]: [system] Successfully activated service 'or
g.freedesktop.hostname1'
Oct  5 10:56:22 debian NetworkManager[1235]: <info>  [1696503382.1234] device (eth0):
state change: ip-config -> ip-check (reason 'none')
```

Logs du noyau :

```
Oct  5 10:22:33 debian kernel: [ 2345.678901] ata1.00: exception Emask 0x0 SAct 0x0 S
Err 0x0 action 0x0
Oct  5 10:22:33 debian kernel: [ 2345.678902] ata1.00: irq_stat 0x40000001
Oct  5 10:22:33 debian kernel: [ 2345.678903] ata1.00: failed command: READ DMA
```

Serveur Web Apache2

- ❑Installation et configuration d'un serveur web Apache2
- ❑Tests effectués avec accès à une page de test.



Conclusion

Cette infrastructure Linux Debian 12 virtualisée intègre une sécurité renforcée avec une segmentation stricte du réseau, un filtrage efficace, et des services essentiels optimisés.

Le projet répond aux exigences de sécurité et de gestion des ressources en environnement virtualisé.

Remerciement

Je tiens à remercier **Mr Decker** pour son accompagnement et ses précieux conseils.